UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

DEFENDANT'S SUPPLEMENTAL MEMORANDUM IN SUPPORT OF HIS MOTION TO DISMISS SUPERSEDING INDICTMENT

Defendant Ryan Harris submits this Supplemental Memorandum in accordance with the Order of this Court, entered October 20, 2011, and in further support of his motion to dismiss the Superseding Indictment and for a change of venue.

I. THE GOVERNMENT'S CASE IS UNSUPPORTED BY CASE LAW AND WOULD DRASTICALLY AND DANGEROUSLY EXPAND THE SCOPE OF CRIMINAL LIABILITY

At the hearing before this Court on October 20, 2011, the government acknowledged that this is a case of first impression. It also acknowledged that earlier efforts by the government to prosecute the sale of modified cable modems, first under the access device statute and then under the wire fraud statute, were abandoned. See United States v. Delorey, 10-cr-00682-JCF-1 (S.D.N.Y.) (charging wire fraud); United States v. Swingler, 09-mj-00033 (S.D.N.Y.) (charging access fraud). The likely reasons are evident here: the conduct at issue is not criminal, and the wire fraud statute is not so malleable as to reach this conduct.

However, throughout its briefing on these issues, the government has repeatedly gone to great pains to try to hide the novelty and reach of this prosecution. Rather than addressing Harris's arguments directly, the government elides critical facts, fails to cite case law supporting

its position, and tries to discourage pretrial resolution of the important issues it has yet to confront. This pattern continues in the government's Supplemental Memorandum filed on November 3, 2011. Additionally, the government's Supplemental Memo states, for the first time, that the government intends to prove Harris's intent by showing that his book included statements that he hated ISPs and believed that there should be no speed limits on internet access. Not only does this argument raise serious First Amendment concerns, it squarely confronts this Court with the concern raised by the First Circuit in Czubinski, namely: that the wire fraud statute should not be used to prosecute behavior simply because it is "offensive to the morals or aesthetics of federal prosecutors." United States v. Czubinski, 106 F.3d 1069, 1079 (1st Cir. 1997). The motivation to crush a vocal critic of ISPs is on full display here.

As in previous briefings, the government's most recent filing asks this Court to accept its version of the facts in the same breath as it miscasts those facts. On pages 2 and 5 of its Supplemental Memorandum, the government suggests that Harris tried to keep his identity a secret. As Harris pointed out in his Reply Brief, he was not attempting to hide his identity, and his book contained his name, picture, and personal details. The government highlights the name of Harris's book, "Hacking the Cable Modem," as a nefarious detail. But this title says nothing about obtaining free or faster internet, instead indicating that the book would show people how to modify a modem as a free-standing piece of technology. Similarly, the government suggests that Harris operated both a "user-feedback forum" and a "bartering platform," when in fact the TCNISO website had only one forum on which individuals could post about anything they desired. Finally, the government has no evidence to support its contention that Harris obtained a stolen MAC address from the forum. The government alleges that there is a forum post in which

Harris asked for a MAC address. MAC addresses are often printed visibly on modems. There is no evidence that Harris obtained a MAC in response to this request, that if he did, the MAC he obtained was stolen, or that harvesting MAC addresses is "stealing" as the government styles it.[1]

The government has not alleged that Harris's conduct – selling firmware – was itself criminal. It instead claims that the firmware was a "criminal tool," an assertion devoid of legal support, at most suggesting that the character of the firmware became so in the hands of users (as a screwdriver becomes a burglarious tool in the hands of a lock picker).[2]

The government has not alleged that Harris knew three of the named users, that he sold anything to the fourth (in the single known communication with this individual, Harris stated that he did not know him and would not allow him to be a forum moderator), or that he spoke with any product users regarding the alleged unlawful use of TCNISO products.[3]

This case, then, is a pure "buyer-seller" one. It is distinguished by the claim that the seller of a legal product may be criminally culpable for the conduct of end users based on product capability. As a proposition of criminal law, this assertion is offered without support and without any acknowledgment that such a rule would make the mere foreseeability of a criminal use of a legal tool sufficient for the prosecution of a seller. Unlike a situation where a person buys a tool for a disclosed criminal purpose (e.g., telling a gun seller you wish to use the hollow point bullets

---

[1] See Defendant's Reply to Government's Opposition (hereinafter Def't Reply), Part I.C.

[2] For further discussion of the government's "criminal tool" argument, see Def't Reply, Part I.C.

[3] For more details regarding Harris's interactions with alleged product users, see Def't Reply, at 2, n.2.

to kill people on a commuter train), this case entails liability for the foreseeable capability of the tool to do the same.

In its Supplemental Memo, the government refers to its prior briefing and asserts that a "robust body of case law" supports the proposition that a supplier can "under certain circumstances" be liable for the criminal conduct of product users. Gvt. Supplemental Memorandum at 4 (dkt #66). In support of this proposition, the government cites a 1986 edition of a treatise. The relevant section in the current version of that treatise, attached as Exhibit A at 6 et seq., discusses United States v. Falcone, 311 U.S. 205 (1940) and Direct Sales Co. v. United States, 319 U.S. 703 (1943), cases which support Harris's arguments.[4] See Wayne R. LaFave, 2 Substantive Criminal Law § 12.2(c)(3) (2010). This treatise also cites dictum from a single decision by a state court of appeals in 1967, charging an answering service operator with conspiring with customers who used the service in their activities as prostitutes, that "suggests that 'a supplier who furnishes equipment which he *knows* will be used to commit a serious crime may be deemed from that knowledge alone to have intended to produce the result.'" Id. (quoting People v. Lauria, 251 Cal.App.2d 471, 480 (Cal. App. 2nd Dist. 1967)). The treatise goes on to state that "[t]here do not appear to be any decisions reaching such a result," and a footnote clarifies that "[r]ather, the cases continue to emphasize that knowing aid is not sufficient." Id. & n.144. The state case cited went on to conclude that although the defendant knew that his service had been used by prostitutes, there was insufficient evidence to show that he was engaged in a conspiracy to commit prostitution. Lauria, 251 Cal.App.2d at 482. The court noted that it did "not believe an inference of intent drawn from knowledge of criminal use properly applies to the

[4] For full development of these cases and how they apply here, see Def't Reply, Part I.B.

less serious crimes classified as misdemeanors." Id. at 481. So too here where the alleged thefts of service would frequently fall shy of $100.

In its Opposition to Harris's motion, the government cites only cases in which the defendant had direct knowledge of the conspiracy and in which the defendant participated in the conspiracy directly and personally, and was not merely the supplier of a legal product. See United States v. Brown, 495 F.2d 593, 595 (1st Cir. 1974) (finding defendant liable in conspiracy where he met with co-conspirators to discuss disposition of stolen checks, suggested that forged identification could be useful, and helped to obtain that identification); United States v. Grunsfeld, 558 F.2d 1231 (6th Cir. 1977) (finding chemist liable for supplying manufacturers of illegal drugs where "he promoted the very purposes of the conspiracy rather than merely supplying it").

The "robust" body of law favors defendant even if this were a civil proceeding. Civil liability has recognized boundaries, famously, Chief Judge Cardozo's notion of proximate cause – that an event must be sufficiently related to a legally cognizable injury to be held the cause of that injury. Palsgraf v. Long Island Railroad Co., 162 N.E. 99 (N.Y. 1928). A similar civil law boundary is the idea that the criminal use of a product by a third party is a supervening, intervening event that eliminates any responsibility by the seller for the results of the third party's conduct. These doctrines insulate sellers from liability for the conduct of end users.[5] The criminal law too has boundaries, including the rules that a single sale of an item (even an illegal item, such as narcotics) does not make a conspiracy, that a co-conspirator must share the

[5] For a more extensive discussion of these civil law doctrines and how they shield product sellers, see Def't Reply, Part I.A.

common conspiratorial objective (here the fruits of the use of firmware), and that the universe of purchasers of an item (even an illegal one) are not, without more, co-conspirators. This case ignores these boundaries, offering a host of premises at variance with well-developed law, including the following:

- A seller of a legal product may be criminally culpable for end-user conduct, even of unknown individuals.
- Culpability can arise from a single sale (despite well-established doctrines that a single sale does not create a conspiracy, and that an aider must have knowledge of and a stake in a specific transaction.)
- A seller may aid and abet a product user based on the capability of a product that is legal to sell.
- A conspiracy can join all users even if they share no common objective (despite formidable case law that conspiracies are not established solely by the common interest in selling or using an item, even an illegal one).
- Product users, who act independently of each other, may be joined in a conspiracy by the existence of an online forum (despite a statute establishing that a forum moderator is not responsible for the content posted on the forum).

As Harris has briefed already, each of these propositions is erroneous.[6] Most conspicuously, as Harris pointed out in his reply, the government has not directed the Court to any cases showing that the seller of a legal product is criminally liable for the conduct of its users.[7] As Harris has highlighted, even in the less demanding realm of civil law, only the publisher of a how-to-kill manual who stipulated to his intent has faced civil consequences, but not the seller of a sure-to-kill bullet or of a how-to-suffocate instructional text.[8] On the criminal side, the boundaries are set firmly by Supreme Court precedent, permitting criminal prosecution

---

[6] See Def't Reply, Part I.B; Defendant's Memorandum in Support of Motion to Dismiss Superseding Indictment, Parts III.B-D.

[7] See Def't Reply, Part I.B-C.

[8] See Def't Reply, Part I.A.

of a drug seller (legally restricted product) but not a retailer of lawful goods to a bootlegger (even with knowledge of the illegal objective). Compare Direct Sales Co., 319 U.S. 703, with Falcone, 311 U.S. 205. In the face of these well-developed standards, the government has not identified any cases imposing criminal liability on a seller based solely on the conduct of product users. It has presented no case law to suggest that such a seller can be criminally liable for the conduct of individuals whom he did not know and with whom he did not communicate.

The hypotheticals discussed during the hearing in this Court involved a seller and purchaser communicating directly about a desired criminal end. No such connection is alleged here. On the contrary, the government admits that, aside from the act of ordering the products, three of the customers never spoke with Harris or any other TCNISO employees. And Harris rebuffed the fourth user when he attempted to talk to Harris about becoming a moderator on the TCNISO forums. There is no allegation that any of these users attempted to or did communicate with Harris about the possibility of getting free or faster internet. Contrast United States v. Patterson, 534 F.2d 1113, 1114 (5th Cir. 1976) (finding seller of illegal "blue box" devices that enabled users to make free phone calls liable where defendant "explained to an undercover telephone company employee that thousands of dollars could be saved by illegally using the 'blue box.' He explained that use of the 'blue box' was illegal, even citing the pertinent statute, and cautioned that the device should be carefully used lest someone discover it. He then demonstrated the 'blue box' to the undercover agent by making several overseas calls to information operators."). Nor is there any allegation that the four users identified in the indictment posted information on the TCNISO forum. The government's case rests solely on the creation and capability of a legal, commercial product.

Finally, it is unclear how the government proposes to distinguish this case from the activities of companies like Microsoft, Google, Rapid7, and Smith & Wesson.[9] Surely those corporations would be horrified to learn that if users of their products misbehave, they may be criminally liable for the users' conduct even though they have long been safe from civil liability in such situations. Especially in the field of technology, innovation often comes from all sides. The partnership between Steve Jobs and Steve Wozniak, for example, was inspired by the work of "phone phreaks," individuals who explored and exploited the inner workings of the phone system, using their knowledge to make free phone calls. See Ron Rosenbaum, "Steve Jobs and Me," October 7, 2011, available at http://www.slate.com/articles/technology/the_spectator/2011/10/steve_jobs_and_the_little_blue_box_how_ron_rosenbaum_s_1971_arti.html. This ostensibly undesirable behavior inspired the development of Apple, the leader in the personal computing revolution of recent years. Labeling technology as "good" or "bad" before its potential has been developed is often counterproductive, and preventing companies from exploring all innovations can only hamper discovery and slow the rate of progress. A ruling from this Court that criminal liability can flow from the capabilities of a legal product would reshape criminal law by imposing a strict liability risk for any product going to market, and provide a powerful tool for prosecutors to pick and choose bad from good technology and prosecute accordingly.

Nor can the wire fraud statute broaden the scope of culpability to criminalize Harris's conduct. In order to prove a wire fraud charge, the government must establish, inter alia, the existence of a scheme to defraud and that Harris had the specific intent to defraud. See United

[9] For further discussion of this argument, see Def't Reply, Part II.

States v. Vazquez-Botet, 532 F.3d 37, 63 (1st Cir. 2008). Here, the government has failed to allege the existence of a scheme in which Harris and the users of his products participated. Once Harris sold a product he was indifferent to how a customer might use it, just as customers were indifferent to what Harris did in the future and to how other individuals used the product. Customers could have used the firmware at issue in at least five ways: 1. to get free service; 2. to get faster service; 3. to conceal their identity; 4. to diagnose connectivity problems; or 5. to connect to the internet normally with any modem. Of these possibilities, the second and third are violations of the terms of service, that is, violations of conditions set by provider for use of its product, which courts have proven unwilling to enforce as predicates for criminal prosecution. See United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (false representations to MySpace about identity not actionable under the Computer Fraud and Abuse Act). The last two potential users are not crimes by anyone's estimation. Since there is no allegation that Harris knew of any customer's planned use of the firmware, there is no proof that Harris and the customers were participating in a scheme, or that Harris specifically intended to defraud anyone. The only possible liability, then, arises within the well-established boundaries of aiding and abetting and conspiracy law, and a wire fraud charge does not lower the threshold of proof.

II. THESE ISSUES DEMAND PRETRIAL RESOLUTION

The fundamental facts here are few. In connection with three of the four named users, the government claims that each purchased firmware through TCNISO's website. These individuals lived in Massachusetts, and the products they ordered were allegedly shipped to them in Massachusetts from TCNISO's headquarters California. One or more of these persons allegedly accessed TCNISO's website and read the postings in the forum. The forum was a publicly

available, web-based chat site, where anyone could post anything. By statute, internet service providers are not responsible for third-party content that they host. 47 U.S.C. § 230(c)(1). The government has not alleged that Harris posted about allegedly illegal activity,[10] only that others did, and that some product users accessed these posts. As to the fourth user named in the indictment, there is evidence that he communicated with Harris. The sole communication the government has identified between Harris and this individual is a conversation in which the user asked to become a forum moderator, but Harris rebuffed him and told him that he did not know him. The government alleges that this individual used, but did not purchase, TCNISO products. There is no evidence that he ever told anyone how he intended to use these products.

In each instance, the facts distill to this: a person allegedly obtained firmware made by a company of which Harris was a principal, accessed a forum containing information about the product, and used the product to get free or enhanced internet service. Under these circumstances, Harris submits that no case imposes criminal liability, and no sound reason exists to cause him to continue to face unprecedented and unsupported criminal charges in a court far from his home.

This conclusion is supported by the cases cited by this Court. In United States v. Barletta, the government sought to have the appellate court compel the district court to determine, prior to trial, whether a certain tape recorded conversation could be admitted at trial. 644 F.2d 50, 51-52 (1st Cir. 1981). The case required the court to determine "when if ever may a district court defer its ruling until trial." Id. at 54. After examining the text of Rule 12, the court explained that

[10] The government has pointed to a single post by Harris, seeking a MAC address for a given area. MAC addresses are not legally protected, and this post does not explain Harris's need for the information or discuss allegedly illegal activity. See Def't Reply at Part. I.C.

Rule 12 "vest[s] discretion in the district court to decline to rule pretrial on many motions, but at the same time requir[es] it to rule in a limited class of cases." Id. at 57.

> Specifically, a district court must rule on any issue entirely segregable from the evidence to be presented at trial, but may in its discretion defer a ruling on any motion that requires trial of any nontrivial part of "the general issue" that is, the presentation of any significant quantity of evidence relevant to the question of guilt or innocence on the ground that it requires trial of the general issue for purposes of 12(b).

Id. at 57-58. Harris's motion to dismiss falls into the first category: the issues he presents can be determined without this Court making findings on the evidence that will be admitted at trial. For the purposes of this motion, Harris asserts that even assuming all of the facts alleged by the government, the indictment does not allege a crime, and the charges must be dismissed. While the government asserts that these issues are not appropriate for pre-trial determination because ruling on them would require pre-trial fact-finding, the fundamental facts for at least three of the four persons appear undisputed for purposes of this motion (that each bought firmware and none communicated with Harris), and that the fourth did not communicate with Harris on the subject of his use of firmware. It certainly appears, from the government's frank statements of the scope of its proof, that there are no factual disputes which should impede pretrial consideration.

Additionally, even if this Court concludes that some preliminary fact finding is necessary to decide Harris's motion, such an action is appropriate. In United States v. Salemme, one defendant filed a motion to dismiss arguing that the government had promised him immunity. 1997 WL 810057, at *1 (D. Mass. 1997). This Court granted the defendant's request for a pretrial hearing on this motion and noted that the defendant's claim was a legal issue to be decided by the Judge and that a court should "decide a pretrial motion prior to trial unless there is

good cause to defer a decision." Id. at *1. This Court noted that "Federal Rules of Criminal Procedure '12(e) and (g) clearly envision that a district court may make preliminary findings of fact necessary to decide the questions of law presented by a pretrial motion so long as the court's findings on the motion do not invade the province of the ultimate finder of fact.'" Id. (quoting United States v. Jones, 542 F.2d 661, 664-65 (6th Cir. 1976)). In this case, not only is there no good cause to defer decision on Harris's motion to dismiss, there is good cause to resolve the issues in advance of trial. The allegations raise substantial legal issues of first impression that should be examined long before the case goes to the jury. Harris does not seek the resolution of factual disputes, but rather meaningful legal review of this unprecedented case that departs dramatically from established legal principles.

In United States v. Jalbert, the defendant filed a motion to dismiss based on outrageous government behavior. 242 F.Supp.2d 44, 45 (D. Me. 2003). The court determined that it had good cause for deferring ruling on this motion because the defendant "had not proffered any particularized evidence of outrageous conduct . . . nor requested an evidentiary hearing. Lacking a developed factual record, the Court is ill-equipped to address Defendant's motion at the present time." Id. at 46. Similarly, in United States v. Djokich, the defendant filed a motion to dismiss arguing that the government had improperly manufactured jurisdiction. 2010 WL 276336, at *1 (D. Mass. 2010). This Court declined to resolve this issue before trial, because doing so would require the Court to hear most of the trial evidence, "[s]pecifically . . . evidence of the sequence and substance of the communications and transactions between the defendants and the government's agents." Id. at *1. Unlike in Jalbert and Djokich, this Court has all of the facts that it needs to decide Harris's pretrial motion, and Harris has requested a hearing. At this stage,

Harris argues that the case should be dismissed even if all of the facts alleged by the government are assumed to be true. Accordingly, there is need to wait for the factual record that a trial would produce, and such reasoning does not provide good cause to defer ruling on Harris's motion.

With this indictment the government has waded into uncharted and potentially dangerous waters. It is in the interest of judicial economy to examine these issues before trial to ensure that the government has alleged a potential crime before a lengthy trial commences. Additionally, the legal flaws that plague this case also make venue improper in this district, and if this Court declines to consider the issues pretrial, Harris will be forced to stand trial in this district, potentially in violation of his right to proper venue. These factors weigh in favor of pretrial resolution, and defendant asks that this Court resolve Harris's motion pretrial.

III. CONCLUSION

For the foregoing reasons, Harris urges this Court to dismiss the charges against him before trial. In the alternative, he seeks transfer of the case to the Eastern District of California.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on November 4, 2011.

/s/ Charles P. McGinty

Charles P. McGinty